Universidad de Santiago
Facultad de Ciencias
Departamento de Matemática y Ciencia de la Computación

Introducción a la Criptografía Moderna
Laboratorio 1

Prof: Rodrigo Abarzúa

March 16, 2017

1 DES: Data Encryption Standard

EL Data Encryption Standard (DES) es el más popular algoritmo de cifrado de bloques. Aún cuando es considerado inseguro para algunos ataques, dado que el conjunto de claves es muy pequeño, se sigue utilizando en algunas aplicaciones. Además, en la actualidad se considera que al aplicar 3 veces el algoritmos DES (conocido como 3DES o triple DES) resulta ser un algoritmo de cifrado muy seguro. El estudio del algoritmo DES es importante ya que ha inspirado a varios algoritmos simétricos de cifrado actuales. Como el algoritmo DES es un cifrador simétrico entonces utiliza la misma clave para encriptar como desencriptar.

1.1 Función f DES

La función f juega una papel fundamental para la seguridad del DES.

- En la ronda i la función f toma la mitad R_{i-1} y la clave derivada k_i. La salida de la función f es de $32-$bits y usada con un XOR para encriptar la mitad izquierda L_{i-1} .
- La mitad R_{i-1} de largo de $32-$bits es "expandida" a un vector de bits de largo de $48-$bits de acuerdo a la función de expansión E.
- $E(R_{i-1})$ consiste en los 32 de R_{i-1}, permutado de cierta manera, con 16 bits aparecen dos veces, a través de la siguiente tabla de selección de bits:

Función de Expansión E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

- El cálculo $E(R_{i-1})$ de 48−bits es XOR con la clave k_i (es decir $E(R_{i1}) \oplus k_i$) y el resultado es concatenado en en un vector de 84 posiciones de 6−bits cada uno, es decir, $B = B_1B_2B_3B_4B_5B_6B_7B_8$.
- Cada uno de estos subvectores B_i de largo de 6−bits y son ingresados en 8 cajas de sustitución conocidas como S−boxes y denotadas como $S_1, \ldots, S_8$, es decir, $S_i(B_i)$ para $i = 1, \ldots, 8$.
- Estas cajas de sustitucin S_i son arreglos fijos de $4 * 16$ cuyas entradas son valores enteros entre $0, \ldots, 15$.
- Cada B_i de largo 6−bits, digamos $B_i = b_1b_2b_3b_4b_5b_6$, es transformado por la caja S_i como $(S_i(B_i))$:
  - Los bits b_1b_6 determina la representación binaria de la fila r de S_i $(0 \leq r \leq 3)$.
  - Los cuatro bits $b_2b_3b_4b_5$ determina la representación binaria de la columna c de S_i $(0 \leq c \leq 15)$.
  - Entonces $S_i(B_i)$ se define como entradas $S_i(r, c)$ escritas en representación binaria que es un vector de bits de largo 4.

  Las cajas S_i son :

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2															
15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3															
10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4															
7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5															
2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6															
12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7															
4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8															
13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

- La salida $C_i = S_i(B_i)$ (con $1 \leq i \leq 8$) $4-$bits para cada C_i.
- Luego para finalizar la función f, el arreglo de bits $C = C_1C_2C_3C_4C_5C_6C_7C_8$ tiene largo de $32-$bits $(4*8)$ y se le aplica una permutación fija P, dada por:

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

2 Laboratorio:

Considere el problema de implementar la función f del DES.

2.1 Se solicita:

1. Implementar la función f del DES. Dados las variables explicadas anteriormente.
2. Implementar en lenguaje C un algoritmo para la función f.
3. Se debe entregar:
   - Código fuente del algoritmo.
   - Informe en LaTeX que contiene:
     - Algoritmo implementado.
     - Formulación del experimento.
     - Curvas de desempeño de resultados.
     - Conclusiones.